ABSTRACT

Methods are disclosed for improving public key cryptography schemes, such as RSA and its variants, to allow for decryption of messages using less than all of the prime factors of the modulus that is used for encryption of said messages.

5